From: Mary Thien Hoang
To: Rebecca Fenneman; Paul A. Schofield
Subject: FYI: Feds may weigh changes to information security requirements
Date: Thursday, January 6, 2011 7:09:14 AM
Attachments: Memorandum for the Heads of Executive Departments and Agencies 01032011.pdf

---

Good morning Rebecca and Paul:

In case you guys were not aware of this…..mot sure if OMD or Mary M. in OHR is aware.

http://www.nextgov.com/nextgov/ng_20110105_6716.php?oref=rss?zone=NGtoday

Feds may weigh changes to information security requirements

BY ALIYA STERNSTEIN 01/05/2011

Before a military employee allegedly leaked a mountain of classified documents to WikiLeaks, reportedly by downloading data to a music CD, the White House had been in the middle of updating rules on reporting agency network weaknesses. Obama officials have not said whether they will revise the reporting guidelines further after agencies complete self-evaluations of their classified information protections.

Under Office of Management and Budget rules issued in April 2010, chief information officers have been working within the confines of the 2002 Federal Information Security Management Act to shift to an automated process for complying with the law's paperwork requirements. Instead of requiring managers to check boxes in reports to indicate compliance with security protocols, special software will continuously collect metrics on the status of controls so that CIOs have a more accurate and comprehensive view of vulnerabilities. Starting this month, CIOs must update the Homeland Security Department monthly, rather than quarterly, on their overall security postures by feeding summaries of these assessments to a central, governmentwide inbox called CyberScope.

Allan Paller, director of research at the SANS Institute, a computer security think tank, suggested OMB refine the April FISMA guidance by directing CIOs to first automate and monitor what a consortium of nonprofit and agency specialists have defined as the 20 most critical FISMA controls.

The top 20 include hardware and software configurations, wireless device control, and data leakage protection. Attempting to tackle the nearly 150 standard controls all at once could dilute agencies' time, money and ultimately security, Paller said. "The 20 critical controls make the defense against that type of attack extremely high priority," he added.

OMB on Monday issued separate guidelines (see attachment) to agency heads on safeguarding classified information that require a one-time report on compliance with information assurance controls, as well as adherence to other existing policies, such as steps to evaluate the trustworthiness of personnel. Agencies were told to conduct similar inspections regularly but, as of now, are not required to continue reporting on these self-assessments. White House officials on Wednesday said

they have not yet announced if they will call for additional reports on the ongoing self-evaluations.

Other security specialists discouraged the government from rushing to change the current OMB requirements for reporting on computer security in response to the WikiLeaks breach.

"There are pieces in [FISMA] that if properly followed by the letter of the law, and the regulations, greatly minimize the risk of things like this happening," said Hord Tipton, executive director of (ISC)2, a nonprofit group that certifies and trains information security professionals. "I think we have quite adequate hardware and technology to deal with it."

But the government must evaluate more closely the people it tasks to follow the rules, cautioned Tipton, who served for five years as the Interior Department's chief information officer.

"All of this depends upon people and people that we trust. We have to take an introspective look at how much we should trust people," he said. Also, "We might not have enough capable people to configure the technology. . . . You've got to recognize that all data is not the same and we're drowning in it. If we're going to live in a sea of data like this, we have to hire people who know how to deal with it."

Mary Thien Hoang
Federal Maritime Commission
Office of the General Counsel
800 N. Capitol Street, NW
Washington, DC 20573

Office Dial: (202) 523-5740
Direct Dial: (202) 523-5782
Facsimile: (202) 523-5738
Email: MHoang@fmc.gov
Website: www.fmc.gov